УДК 513.6:517.1:519.48

Белецкий А. Я.
Национальный авиационный университет, Киев, Украина

ОБОБЩЕННЫЕ МАТРИЦЫ ГАЛУА В ПРОТОКОЛАХ ОБМЕНА КЛЮЧАМИ ШИФРОВАНИЯ

DOI: 10.14308/ite000569

Рассмотрены методы построения матричных протоколов формирования секретных ключей шифрования легализованными абонентами открытых коммуникационных сетей. В основу протоколов обмена ключами положены алгоритмы ассиметричной криптографии. Решение проблемы предполагает вычисление односторонних функций и базируется на использовании обобщенных матриц Галуа, связанных отношением изоморфизма с образующими элементами, и зависящих от выбранных неприводимых полиномов, порождающих матрицы. Разработан простой способ построения обобщенных матриц Галуа по методу диагонального заполнения. С целью устранения изоморфизма матриц Галуа и образующих их элементов, ограничивающий возможность построения односторонних функций, матрицы Галуа подвергаются преобразованию подобия, осуществляемых с помощью перестановочных матриц. Предлагается вариант организации алгебраической атаки на протоколы обмена ключами шифрования и обсуждаются варианты ослабления последствий атаки.

Ключевые слова: *протокол обмена ключами, односторонние функции, обобщенные матрицы Галуа, отношение изоморфизма, алгебраическая атака на протокол обмена ключами шифрования.*

Постановка проблемы исследования.

Одной из наиболее актуальных задач, решаемой современной криптографией, является формирование секретных ключей шифрования легализованными абонентами открытых коммуникационных сетей или иных открытых каналов передачи информации. Особую остроту приобретает данная проблема в системах управления беспилотными летательными аппаратами (БПЛА), поскольку несанкционированный доступ, например, в радиоканал приема-передачи командно-телеметрической информации сопряжен с риском потери аппарата или может привести к другим тяжким последствиям [1].

Для обмена зашифрованными сообщениями между двумя абонентами криптосистемы необходимо, чтобы обоим участникам обмена доставлялись сохраняемые в секрете ключи шифрования. Технология формирования секретных ключей по открытым каналам связи в случае, когда каждый из двух абонентов сети участвует в генерации этого секретного ключа, носит название *протокола обмена ключами* (ПрОК), являющегося частным случаем *протокола распределения ключей.* Вторым типом протокола предполагается не только выработка секретного ключа шифрования, но и его распределение между всеми абонентами (число которых может превышать два) некоторой легализованной группы открытой коммуникационной сети. И, наконец, в том случае, когда секретный ключ не вырабатывается в протоколе, а приобретается заранее кем-либо из участников группы, то такой протокол носит название *протокола распространения ключей* [2, 3]. Предметом исследования в данной статье являются исключительно протоколы первого типа, то есть протоколы обмена ключами.

Примем следующие соглашения относительно обозначения переменных: матрицы будем выделять жирным шрифтом, над вектор-столбцами – ставить черточки (например, $\bar{V}$), а вектор-строки оставляем в оригинале без черточек.

Анализ последних достижений и публикаций.

Первым протоколом, заложившим основу *ассиметричной* (двухключевой) криптографии, и на ее основе – построения целой серии протоколов обмена ключами шифрования, является ставшим в настоящее время классическим *протокол Диффи-Хеллмана* (DH-протокол или алгоритм), который позволяет двум сторонам, назовем их абонентами A и B, совместно создать общий секретный ключ K, используя незащищенный канал связи [4]. Этот ключ может быть применен для криптопреобразования последующих сообщений с помощью симметричного шифрования.

DH-алгоритмом предусматривается, что абонентам A и B известны открытые ключи p и q, причем $p-$ простое число, а $q-$ примитивный образующий элемент. Абонент A генерирует случайное большое число a, вычисляет значение $N_a = q^a \bmod p$ и направляет его абоненту B. В свою очередь B генерирует случайное большое число b, вычисляет значение $N_b = q^b \bmod p$ и направляет его абоненту A. Далее абонент A возводит полученное от B число N_b в свою случайную степень a и вычисляет значение $K_a = (N_b)^a \bmod p = q^{ba} \bmod p$. Аналогично поступает абонент B, вычисляя $K_b = (N_a)^b \bmod p = q^{ab} \bmod p$. Очевидно, что оба абонента получают одно и тоже число (ключ шифрования) K, поскольку $K_a \equiv K_b$.

Главной недостаток протокола DH заключается в том, что, во-первых, он не защищен от атаки "человек посередине" [5] и, во-вторых, требует для своего построения достаточно больших простых чисел p, генерация которых и проверка "на простоту" сопряжена, зачастую, со значительными ресурсными затратами. Поэтому были предложены и другие варианты протоколов обмена ключами, среди которых отметим так называемые матричные аналоги алгоритма Диффи-Хеллмана, а именно, алгоритмы Ероша-Скуратова [6,7] и Мегрелишвили [8]. Хотя перечисленные протоколы также не защищены от атаки типа "человек посередине", но, по сравнению с DH-протоколом, гораздо проще в программно-аппаратной реализации.

В работах [6,7] предлагается строить блочные криптографические шифры на основе обратимых матриц над полем *GF*(2). Если X, Y – векторы длины n, представляющие собой блоки соответственно открытого и зашифрованного текстов, а $\boldsymbol{M}$ – шифрующая матрица $n-$го порядка, то зашифрование задается уравнением $Y = \boldsymbol{M} \cdot X,$ а расшифрование – уравнением $X = \boldsymbol{M}^{-1} \cdot Y$. Для обмена сеансовыми ключами в системе авторы предлагают использовать протокол Диффи–Хеллмана в циклической группе матриц $\langle \boldsymbol{M} \rangle$, причем матрица $\boldsymbol{M}$ считается общедоступной. Предполагается, что абонент A вырабатывает случайный секретный показатель x, вычисляет матрицу $\boldsymbol{M}^x$ и посылает ее абоненту B. В свою очередь абонент B вырабатывает случайный показатель y, вычисляет матрицу $\boldsymbol{M}^y$ и посылает ее абоненту A. Затем оба абонента возводят полученные матрицы в свои степени и получают общий ключ шифрования $\boldsymbol{M}^{xy} = \boldsymbol{M}^{yx}$. Поскольку мощность группы, образующим элементом которой являются невырожденные двоичные матрицы $\boldsymbol{M}$ (рекомендуемый порядок должен быть не менее, чем 100), велико, то вычисление ключа, как утверждают авторы (кстати, без доказательства), имеет переборную сложность.

Алгоритм (протокол) Ероша-Скуратова (ЕС), так же, как и DH-протокол, не защищен от атаки "человек посередине". Более того оказалось, как показано в [9], что ЕС-протокол является недостаточно криптостойким и секретный ключ шифрования легко взламывается *алгебраической атакой*. Алгебраические атаки на шифры и протоколы

обмена ключами могут быть представлены в виде проблемы решения большой системы булевых алгебраических уравнений, которая следует геометрии и структуре частной криптографической схемы [10]. Более подробные пояснения к методу взлома "алгебраической атакой" протокола Ероша-Скуратова и других рассматриваемых далее матричных протоколов формирования ключей шифрования приводятся ниже по тексту.

Более "продвинутым" по сравнению с ЕС-протоколом является протокол Мегрелишвили [8], суть которого состоит в следующем. В качестве открытых ключей в протоколе принимаются двоичный вектор инициализации V и примитивная матрица $\boldsymbol{M}$ нечетного порядка n. Абонент A генерирует случайный показатель x, вычисляет вектор $V_a = V \cdot \boldsymbol{M}^x$ и посылает его абоненту B. В свою очередь абонент B генерирует случайный показатель y, вычисляет вектор $V_b = V \cdot \boldsymbol{M}^y$ и посылает его A. Далее абонент A вычисляет ключ $K_a = V_b \cdot \boldsymbol{M}^x = V \cdot \boldsymbol{M}^{y+x}$, а B – ключ $K_b = V_a \cdot \boldsymbol{M}^y = V \cdot \boldsymbol{M}^{x+y}$. Совершенно очевидно, что после завершения протокола обмена данными оба абонента получают одинаковый секретный ключ $K = K_a \equiv K_b$.

Алгоритм формирования примитивных матриц $\boldsymbol{M}_n$, где $n-$порядок матрицы, в протоколе Мегрелишвили достаточно простой и поясняется следующей схемой вычислений

$$\boldsymbol{M}_1 = 1, \quad \boldsymbol{M}_3 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & \boldsymbol{M}_1 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \boldsymbol{M}_5 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & & & & 0 \\ 0 & & \boldsymbol{M}_3 & & 1 \\ 1 & & & & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}, \ \ldots \qquad (1)$$

Для произвольного нечетного значения n матрицу Мегрелишвили $\boldsymbol{M}_n$ можно представить соотношением

$$\boldsymbol{M}_n = \begin{pmatrix} 1(01)^{[n/2]} \cdot \begin{bmatrix} 1 \\ x^{-1} \\ \ldots \\ x^{-[n/2]} \end{bmatrix} \\ 0(10)^{[n/2]} \cdot \begin{bmatrix} x^{[n/2]} \\ \ldots \\ x \\ 1 \end{bmatrix} \end{pmatrix}, \qquad (2)$$

в котором показатель степени $[b]-$целая часть дробного числа b; $a \cdot x^k -$круговая прокрутка $n-$битного числа a на k разрядов по часовой стрелке, $a \cdot x^{-k} -$ круговая прокрутка числа a против часовой стрелки; и, наконец,

$$(c)^k = \underbrace{c, c, \ldots, c}_{k \text{ раз}}.$$

Отметим, что протокол Мегрелишвили, как и ЕС-протокол, не свободен как от атаки "человек посередине", так и алгебраической атаки. Кроме того, и это следует из (1) и (2), матрицы Мегрелишвили $\boldsymbol{M}_n$, $n = 1, 3, 5, \ldots$, являются матрицами исключительно нечетного порядка, что может вызвать определенные затруднения в криптографических приложениях.

Но если в ЕС-протоколе на этапе формирования ключа шифрования легализованные абоненты сети обмениваются пакетами (матрицами бинарных данных), порядок которых составляет n^2, где $n-$порядок обменных матриц, то в протоколе Мегрелишвили порядок передаваемых данных (бит) понижается до значения n, являющегося порядком вектора инициализации V, совпадающего с порядками векторов V_a и V_b, которыми обмениваются абоненты коммуникационной сети A и B. И в этом проявляется одно из преимуществ протокола Мегрелишвили по сравнению с протоколом Ероша-Скуратова.

Обмен секретными ключами шифрования решается, как правило, с помощью так называемых *односторонних* (*однонаправленных*) *функций* [11]. Вычисление односторонних функций в одном направлении не представляет особых затруднений, тогда как нахождение обратной функции требует значительных вычислительных ресурсов. В частности, стойкость асимметричного RSA криптографического шифра, популярном алгоритме, который часто используется для построения односторонних функций и протоколов обмена ключами, основывается на факторизации больших чисел и требует экпоненциального по числу знаков факторизуемого числа операций [12]. Основной недостаток RSA-протоколов, ограничивающий их применение в *системах обмена ключами шифрования*, состоит в их низком быстродействии, обусловленном необходимостью выполнения вычислений над двоичными операндами большой размерности, достигающих нескольких Кбит.

В связи с вышеизложенным, проблема разработки эффективных протоколов обмена ключами шифрования не снижает своей остроты и продолжает оставаться актуальной.

Постановка задачи исследования.

В данной статье разрабатываются способы формирования односторонних функций, базирующийся на так называемых *обобщенных матрицах Галуа* (ОМГ), и предлагаются на их основе алгоритмы построения ОМГ-ПрОК, ориентированные на применение в системах оперативной смены ключей шифрования в каждом сеансе связи между наземным пунктом управления (НПУ) и бортовой аппаратурой БПЛА. Под *сеансом связи* понимается передача по радиоканалу одиночного пакета информации в направлении НПУ – борт БПЛА или наоборот.

Понятийно-терминологические определения.

При изложении какого-либо раздела области знаний принципиальным является соглашение относительно определения основных терминов (понятий), используемых в научных статьях, монографиях, учебных пособиях и т.д. При этом следует придерживаться правила, согласно которому определение термина должно приводиться в соответствии со стандартом, если таковой существует, или в формулировке, общепринятой в научной или технической литературе.

Термин *матрицы Галуа*, как и биективно связанные с ними *матрицы Фибоначчи*, заимствованы из теории помехоустойчивого кодирования и криптографии [9], в которых широко применяются генераторы бинарных псевдослучайных последовательностей (ПСП) в конфигурациях Галуа и Фибоначчи, построенные на линейных регистрах сдвига (ЛРС или РС) с линейными обратными связями (ЛОС). Известно [13], что для того чтобы ЛРС являлся генератором ПСП максимального периода, соответствующий полином обратной связи должен быть *примитивным полиномом* (ПрП). Пример генератора Галуа восьмого порядка, формирующего ПСП максимального периода, показан на рис. 1.

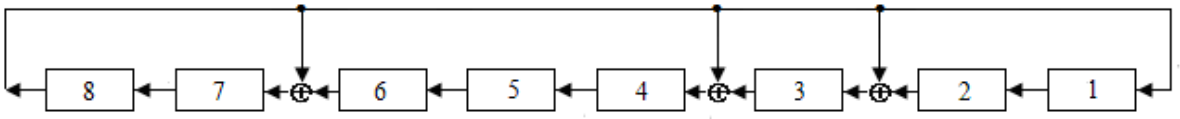

Рис. 1. Структурная схема генератора ПСП по схеме Галуа над ПрП $f_8 = 101001101$.

Классический генератор Галуа, представленный на рис. 1, сопоставляет каждому ненулевому элементу поля $GF(2^8)$ соответствующую степень примитивного элемента

$\theta = 10$ по модулю ПрП $f_8 = 101001101$. В качестве элементов памяти линейных регистров используют, как правило, $D-$триггеры, уровень сигнала на выходе которых (0 или 1) после подачи синхроимпульса повторяет уровень сигнала, подведенного к входу триггера. Блок $\oplus$ в ЛРС осуществляет операцию сложения по модулю 2 (операцию XOR).

Как следует из структурной схемы генератора (рис. 1), обратные связи в классических генераторах (регистрах) Галуа однозначно определяются выбранным ПрП f_n степени n и формируются таким способом: отклики каждого разряда ($D-$триггера) ЛРС поступают на входы последующих разрядов, являясь для них функциями возбуждения. Кроме того, отклик старшего разряда регистра подается (по схеме XOR) на входы тех и только тех разрядов, номера которых совпадают с номерами ненулевых мономов ПрП. При этом младшему моному, расположенному справа полинома f_n, как и младшему (правому) разряду регистра на рис. 1, соответствует номер 1.

Двоичные ПрП f_n порождают поля $GF(2^n)$, минимальный примитивный элемент которых θ равен 10. Последовательность степеней любого примитивного элемента θ поля Галуа по модулю ПрП f_n, то есть $\theta^k (\mathrm{mod}\, f_n)$, $k = 0,1,\ldots$, формируют последовательность максимальной длины ($m-$последовательность). Фрагмент такой последовательности для полинома $f_8 = 101001101$ внесен в табл. 1.

Таблица 1.

Фрагмент последовательности степеней элемента $\theta = 10$ *по модулю* $f_8 = 101001101$

Степень	Разряды регистра							
k	8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	1	0
2	0	0	0	0	0	1	0	0
3	0	0	0	0	1	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	1	0	0	0	0	0
6	0	1	0	0	0	0	0	0
7	1	0	0	0	0	0	0	0
8	0	1	0	0	1	1	0	1
9	1	0	0	1	1	0	1	0
10	0	1	1	1	1	0	0	1
…	…	…	…	…	…	…	…	…
254	1	0	1	0	0	1	1	0
255	0	0	0	0	0	0	0	1

Непосредственной проверкой легко убедиться в том, что ЛРС (рис. 1) с обратными связями, образуемыми ПрП f_8, порождает последовательность состояний регистра, совпадающую с $m-$последовательностью, частично показанной в табл. 1.

Классические матрицы Галуа.

Каждый линейный РСЛОС-генератор ПСП максимального периода, может быть представлен эквивалентной ему примитивной матрицей Галуа $\boldsymbol{G}$, формирующей ту же самую $m-$последовательность, что и РС-генератор ПСП. Обозначим через $\boldsymbol{G}_f^{(n)}$ двумерную матрицу Галуа $n-$го порядка над неприводимым полиномом (НП) f_n, совсем не обязательно являющимся ПрП. С помощью $\boldsymbol{G}_f^{(n)}$ введем рекуррентное вычисление состояний $S(t)$ регистра в дискретные моменты времени t:

$$S(t) = S(t-1) \cdot \boldsymbol{G}_f^{(n)},\ t = 1,2,\ldots,\ S(0) = 00000001. \qquad (3)$$

Вектором $S(0)$ в (1) выделяется нижняя строка (припишем ей номер 1) матрицы $\boldsymbol{G}_f^{(n)}$. Следовательно, в нижней строке матрицы $\boldsymbol{G}_f^{(8)}$ необходимо записать (согласно табл. 1) значение $S(1) = 10$, совпадающее с минимальным образующим элементом (ОЭ) $\theta = 10$ поля $GF(2^8)$ над ПрП $f_8 = 101001101$.

Соотношением $S(2) = S(1) \cdot \boldsymbol{G}_f^{(8)}$ выделяется вторая (снизу) строка матрицы $\boldsymbol{G}_f^{(n)}$, которая, по данным табл. 1, вне зависимости от ПрП, или просто НП, должна быть равна 100. Продолжая вычисления, приходим к матрице

$$\boldsymbol{G}_f^{(8)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \cdot \qquad (4)$$
$$8\ \ 7\ \ 6\ \ 5\ \ 4\ \ 3\ \ 2\ \ 1$$

В соответствии с выражением (3) алгоритм синтеза классических матриц Галуа, подобных (4), может быть сформулирован следующим образом. Пусть f_n – векторная форма ПрП степени n такая, что

$$f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\},\ u_i \in \{0,1\},\ i = \overline{1, n-1}, \qquad (5)$$

и $\theta = 10$ – минимальный ОЭ поля $GF(2^n)$ над ПрП f_n. Поместим ОЭ 10 справа в нижней строке матрицы Галуа и заполним элементы матрицы, придерживаясь простого правила. Поставим единицы в элементах диагонали, расположенной ниже главной диагонали матрицы, а в оставшихся элементах матрицы $\boldsymbol{G}_f^{(n)}$, кроме верхней строки, запишем нули. В верхней строке матрицы следует ожидать появления $(n+1)$–битного вектора 100…0. Но это недопустимо, так как порядок матрицы равен n. Приведя такой вектор к остатку по модулю f_n, приходим к тому, что в верхней строке матрицы $\boldsymbol{G}_f^{(n)}$ следует разместить ПрП f_n в конфигурации (3), исключая его старшую единицу, т.е. n–битный вектор $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

На основании предложенного метода, назовем его *методом диагонального заполнения*, получим общую форму *классической матрицы Галуа* n–го порядка

$$\boldsymbol{G}_f^{(n)} = \begin{bmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}. \qquad (6)$$

Матрицы $\boldsymbol{G}_f^{(n)}$ над ПрП f_n взаимно однозначно связаны с матрицами Фибоначчи $\boldsymbol{F}_f^{(n)}$ оператором $\perp$ *правостороннего транспонирования* [14]

$$\boldsymbol{G} \overset{\perp}{\longleftrightarrow} \boldsymbol{F}$$

т.е. транспонирования относительно вспомогательной диагонали.

$$\boldsymbol{F}_f^{(n)} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{bmatrix}. \qquad (7)$$

Матрицы (6) и (7) являются частными случаями фробениусовой [15, 16] канонической матрицы

$$\boldsymbol{F} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & 0 & -a_2 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

Такая матрица называется также *сопровождающей для многочлена*

$$f(x) = x^n - \alpha_{n-1}x^{n-1} - \alpha_{n-2}x^{n-2} - \cdots - \alpha_0 .$$

Если $f(x) = f_n(x)$ есть примитивный двоичный полином $n-$й степени, то

$$f_n(x) = x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_0 . \qquad (8)$$

Матрица Фробениуса, соответствующая ПрП (8), имеет вид

$$\boldsymbol{F} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & a_0 \\ 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & \cdots & 0 & 0 & a_2 \\ \cdots & \cdots & \ddots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & a_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & a_{n-1} \end{bmatrix}. \qquad (9)$$

Транспонируя матрицу (9) относительно вспомогательной диагонали, приходим к матрице

$$\boldsymbol{G} = \begin{bmatrix} \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_1 & \alpha_0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \qquad (10)$$

Матрицы (6) и (7), первородными которых являются матрицы (10) и (9) соответственно, используются для построения РСЛОС по схемам Галуа и Фибоначчи над

ПрП (8). Именно такие матрицы $\boldsymbol{G}$ и $\boldsymbol{F}$ будем называть *матрицами Галуа и Фибоначчи*. На основе этих матриц можно построить обобщенные матрицы Галуа и Фибоначчи для любого элемента ω поля $GF(2^n)$ над неприводимым полиномом f_n.

Генератор ПСП в конфигурации Фибоначчи формирует бинарную $m-$последовательность ПСЧ, обладающую теми же самыми статистическими свойствами, что и последовательность чисел, формируемая генератором Галуа. Поэтому ограничимся в дальнейшем рассмотрением только лишь матриц Галуа.

Обобщенные матрицы Галуа.

В данном разделе статьи предлагается алгоритм построения матриц Галуа $\boldsymbol{G}_{f,\omega}^{(n)}$, в качестве образующих элементов которых применяются элементы $\omega \geq p = 10$ поля $GF(p^n)$ над произвольными неприводимыми полиномами f_n (совсем не обязательно примитивными) степени n.

Введем предварительно определение обобщенных матриц Галуа (ОМГ).

Обобщенными будем называть матрицы Галуа $\boldsymbol{G}_{f,\omega}^{(n)}$, образующий элемент которых ω совсем не обязательно является примитивным элементом θ поля $GF(p^n)$ характеристики p, порождаемого произвольным неприводимым полиномом f_n степени n.

Синтез обобщенных матриц Галуа $\boldsymbol{G}_{f,\omega}^{(n)}$ осуществляется выше введенным методом диагонального заполнения и сводится к таким действиям. В нижней строке синтезируемой ОМГ записывается образующий ее элемент $\omega \geq 10$, являющийся элементом поля $GF(p^n)$ над НП f_n. Разряды строки, расположенные слева ОЭ ω, заполняются нулями. Последующие строки матрицы (снизу-вверх) образуются сдвигом предыдущей строки на один разряд влево, а в освобождающийся правый разряд заносится 0. Если при сдвиге старший ненулевой разряд строки выходит за пределы матрицы, то векторы, отвечающие таким строкам, приводятся к остатку по модулю f_n и, тем самым, строка вновь становится n разрядной.

Пусть, для примера, $n = 4$, $f_4 = 11111$ и $\omega = 111$. Приходим к обобщенной матрице

$$\boldsymbol{G}_{f,\omega}^{(4)} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad (11)$$

Структурная схема генератора Галуа, отвечающего матрице преобразования (11), показана на рис. 2.

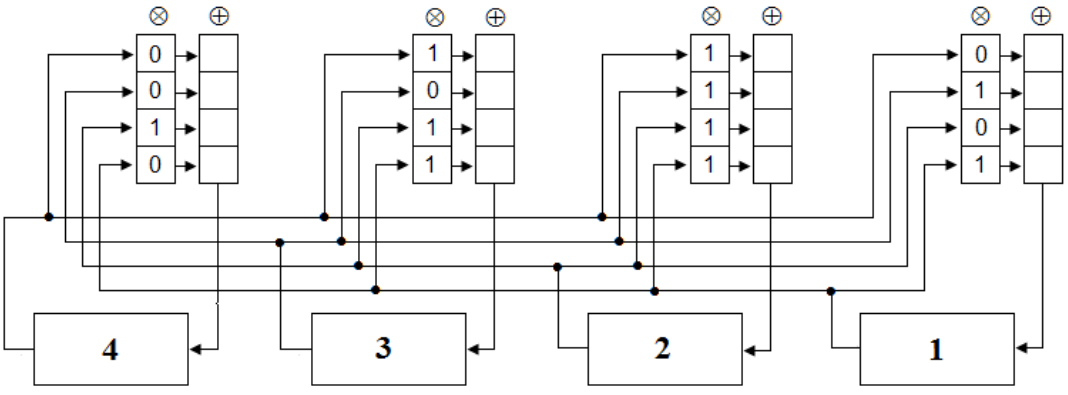

Рис. 2. Структурная схема обобщенного генератора ПСП Галуа.

Вертикально расположенные регистры генераторов, отмеченные сверху символом $\otimes$, реализуют операцию поразрядного умножения, а регистры, отмеченные символом $\oplus$ – операцию сложения содержимого регистра по модулю 2. Из сопоставления значений элементов регистров умножения с элементами матрицы (11) следует, что столбцы обобщенной матрицы Галуа переносятся в соответствующие $\otimes$ – регистры генератора ПСП Галуа.

Изоморфизм матриц Галуа.

Согласно изложенному ранее правилу диагонального заполнения на начальном этапе синтеза матрицы $\boldsymbol{G}_{f,\omega}^{(n)}$ формирующий ее элемент ω размещается в младших (правых) разрядах нижней строки матрицы $n-$го порядка. Последующие строки матрицы (снизу-вверх) образуются сдвигом на один разряд влево предшествующей строки, причем после сдвига в освободившийся правый разряд записывается 0. В том случае, если ненулевой старший элемент сдвигаемой строки выходит за пределы матрицы, то этот $(n+1)-$разрядный $p-$ичный вектор приводится к остатку по модулю f_n. Тем самым строка возвращается в границы матрицы и процесс заполнения ее строк продолжается по уже описанной схеме.

Из теории многочленов (полиномов) одной переменной известно, что умножение произвольного полинома $\omega_k(x)$ степени k на x эквивалентно сдвигу полинома на один разряд влево и, соответственно, увеличению на 1 степени полинома. Другими словами,

$$x\cdot\omega_k(x)\to\omega_{k+1}(x), \tag{12}$$

Воспользовавшись соотношением (12) и, принимая во внимание способ формирования ОМГ, запишем цепочку преобразований:

$$\boldsymbol{G}_{f,\omega}^{(n)}\Rightarrow\begin{bmatrix}x^{n-1}\cdot\omega\\ x^{n-2}\cdot\omega\\ \dots\\ x\cdot\omega\\ x\end{bmatrix}\bmod f_n=\omega\cdot\begin{bmatrix}x^{n-1}\\ x^{n-2}\\ \dots\\ x\\ 1\end{bmatrix}\bmod f_n\cdot \tag{13}$$

Элементами правого вектор-столбца в соотношении (13) являются мономы, которые, будучи представленными в двоичной форме, обращают вектор-столбец в единичную матрицу $\boldsymbol{E}$, т.е.

$$\begin{bmatrix}x^{n-1}\\ x^{n-2}\\ \dots\\ x\\ 1\end{bmatrix}=\begin{bmatrix}1&0&\cdots&0&0\\ 0&1&\cdots&0&0\\ \cdots&\cdots&\cdots&\cdots&\cdots\\ 0&0&\cdots&1&0\\ 0&0&\cdots&0&1\end{bmatrix}=\boldsymbol{E}\text{'} \tag{14}$$

что позволяет сформулировать следующее утверждение.

Утверждение. *Обобщенная матрица Галуа* $\boldsymbol{G}_{f,\omega}^{(n)}$ *порядка* n *над НП* f_n *изоморфна ее образующему элементу* ω*, являющемуся элементом поля* $GF(p^n)$ *характеристики* p

$$\boldsymbol{G}_{f,\omega}^{(n)}\leftrightarrow\omega. \tag{15}$$

Следовательно, согласно выражениям (13) и (14), между ОМГ $\boldsymbol{G}_{f,\omega}^{(n)}$ и ее ОЭ ω существует взаимно однозначное соответствие (*изоморфизм* или *биекция*), отображаемое

отношением (15). Кроме того, легко установить, что изоморфизм (15) приводит к таким последствиям.

Следствие 1. *Для того, чтобы возвести матрицу* $\boldsymbol{G}_{f,\omega}^{(n)}$ *в степень* k, *достаточно вычислить ОЭ* $\omega_k = \omega^k (\mathrm{mod}\, f_k)$ *и по методу диагонального заполнения составить матрицу* $\boldsymbol{G}_{f,\omega_k}^{(n)}$.

Следствие 2. *Минимальное ненулевое значение степени* e, *обеспечивающее равенство* $\left(\boldsymbol{G}_{f,\omega}^{(n)}\right)^e = \boldsymbol{E}$, *совпадает с порядком* ord *элемента* ω, *образующего матрицу* $\boldsymbol{G}_{f,\omega}^{(n)}$.

Следствие 3. *Обобщенная матрица Галуа* $\boldsymbol{G}_{f,\omega}^{(n)}$ *примитивна, если примитивным является образующий её элемент* ω, *т.е. если* $\omega = \theta$.

Следствие 4. *Матрицы* $\boldsymbol{G}_{f,\omega_1}^{(n)}$ *и* $\boldsymbol{G}_{f,\omega_2}^{(n)}$, $\omega_1 \neq \omega_2$, *коммутативны, поскольку являются элементами одной и той же мультипликативной группы максимального порядка* GF^*, *составленной из степеней матрицы* $\boldsymbol{G}_{f,\theta}^{(n)}$, *произвольный образующий примитивный элемент которой* θ *принадлежит полю* $GF(p^n)$ *над НП* f_n.

Следствие 5. *Произвольные алгебраические преобразования (суммирования, вычитания, умножения и деления) над матрицей Галуа или совокупностью матриц Галуа изоморфны таким же преобразованиям над образующими элементами этих матриц.*

Следствие 6. *Множество ОМГ может быть расширено за счет введения подобных матриц Галуа* ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$, *определяемых соотношением*

$$ {}^*\boldsymbol{G}_{f,\omega}^{(n)} = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)} \cdot \boldsymbol{P}, \qquad (16) $$

где $\boldsymbol{P}-$ *матрица преобразования подобия* [17].

В качестве $\boldsymbol{P}-$матриц для преобразования (16) выбраны перестановочные матрицы $n-$го порядка, для которых $\boldsymbol{P}^{-1} = \boldsymbol{P}^{-T}$.

Преобразования (16) существенно расширяют множество обобщенных матриц Галуа ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$ по крайней мере за счет того, что существует $n!$ перестановочных матриц подобия $\boldsymbol{P}$. Но, тем не менее, псевдослучайные последовательности бинарных чисел, формируемые подобными ОМГ ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$, удовлетворяют как постулатам Голомба [18], так и протоколу на основе алгоритма Берлекэмпа-Месси [19] в части поиска *кратчайшего регистра сдвига* с линейной обратной связью для поданной на его вход бинарной последовательности, образуемой ОМГ-генератором.

Односторонние функции и ОМГ-протокол обмена ключами шифрования.

В отличие от ОМГ $\boldsymbol{G}_{f,\omega}^{(n)}$, матрицы ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$, оставаясь коммутативными, утрачивают свойство изоморфизма. Данная особенность подобных матриц Галуа как раз и обеспечивает возможность построения *односторонних функций*, используемых в предлагаемых протоколах обмена ключами абонентами открытых коммуникационных каналов передачи информации.

Введем неформальное определение односторонней (*однонаправленной*) функции [20].

Определение. *Функция* $\varphi: X \to Y$ *называется односторонней, если* $\varphi(x)$ *может быть легко вычислена для каждого* $x \in X$, *тогда как почти для всех* $y \in Y$ *вычисление такого* $x \in X$, *что* $\varphi(x) = y$ *(при условии, что хотя бы один такой* x *существует), является сложным*.

Ниже приведены краткие пояснения к предлагаемому ОМГ-протоколу обмена ключами в открытых сетях (в частности, в каналах радиосвязи НПУ – борт БПЛА). Протоколом предполагается формирование абонентами сети *новой* односторонней функции, посредством которой и вычисляется общий секретный ключ шифрования.

В качестве *открытых ключей* протокола приняты: вектор инициализации V, являющийся $n-$битным вектором; неприводимый двоичный полином f_n степени n и перестановочная $\boldsymbol{P}-$матрица $n-$го порядка. Каждый из абонентов сети A и B вырабатывает *секретные* $n-$*битные ключи* ω_α и ω_β соответственно. Общий секретный ключ K определяется в результате выполнения абонентами таких двух этапов вычислений:

Этап 1. Абонент A генерирует случайный вектор ω_α, находит сначала ОМГ $\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$, затем подобную матрицу ${}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$, вычисляет вектор $\bar{V}_\alpha = {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \bar{V}$ и направляет его абоненту B. Аналогичные операции осуществляет абонент B, определяя вектор $\bar{V}_\beta = {}^*\boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \bar{V}$, который направляет абоненту A. Векторы $\bar{V}_\alpha$ и $\bar{V}_\beta$ как раз и являются теми односторонними функциями φ, которые построены на основе подобных ОМГ.

Этап 2. Абонент A умножает свою секретную матрицу ${}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$ на принятый от абонента B вектор $\bar{V}_\beta$, формируя ключ

$$\bar{K}_\alpha = {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \bar{V}_\beta = {}^*\boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot {}^*\boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \bar{V} = (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{P}) \cdot (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{P}) \cdot \bar{V} = (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{P}) \cdot \bar{V}. \quad (17)$$

Точно такие же вычисления выполняет абонент B, извлекая вектор

$$\bar{K}_\beta = (\boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega_\beta}^{(n)} \cdot \boldsymbol{G}_{f,\omega_\alpha}^{(n)} \cdot \boldsymbol{P}) \cdot \bar{V}. \quad (18)$$

Поскольку ОМГ $\boldsymbol{G}_{f,\omega_\alpha}^{(n)}$ и $\boldsymbol{G}_{f,\omega_\beta}^{(n)}$ коммутативны, из соотношений (17) и (18) следует, что $K_\alpha = K_\beta$, и поэтому оба абонента сети получают одинаковый ключ шифрования K.

Если же вместо подобных матриц ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$ использовать обычные ОМГ $\boldsymbol{G}_{f,\omega}^{(n)}$, то в силу их изоморфизма (15) противник, перехватив векторы $\bar{V}_\alpha$ и $\bar{V}_\beta$, может вычислить секретные ключи ω_α и ω_β, так как в общем случае

$$\bar{V}_\gamma = \boldsymbol{G}_{f,\omega_\gamma}^{(n)} \cdot \bar{V} = \omega_\gamma \cdot \bar{V} \,(\mathrm{mod}\, f_n), \qquad \gamma = \alpha \text{ или } \beta. \quad (19)$$

Ввиду того, что $\bar{V}$ и f_n – известные величины, противник, разрешая равенства (19) относительно ω_γ, вычисляет частные ключи ω_α и ω_β, что и приводит к взлому общего секретного ключа K.

Варианты построения односторонних ОМГ-функций.

Кроме рассмотренного выше способа построения односторонних ОМГ-функций, который назовем "вариантом 1", или *базовым вариантом*, могут быть предложены и другие способы построения односторонних ОМГ-функций. Обозначим через $K1-$секретный ключ шифрования, образуемый первым (базовым) вариантом ОМГ-функций.

Вариант 2, которым предполагается замена вектора инициализации V секретным ключом $K1$ (открытыми остаются ключи f и $\boldsymbol{P}$) и формирование нового секретного ключа $K2$.

Вариантом 3 первоначально осуществляется однозначное формирование по ключу $K2$ секретной перестановочной матрицы $\boldsymbol{P}$ (иллюстрация одного из возможных способов вычисления матрицы $\boldsymbol{P}$ по заданному значению $K2$ приведена ниже), а затем на основании открытого полинома f, секретного вектора V и матрицы $\boldsymbol{P}$ – формирование секретного ключа $K3$.

Рассмотрим один из предлагаемых алгоритмов синтеза перестановочной матрицы $\boldsymbol{P}$ на примере матрицы $n-$го порядка, полагая $n=8$. Пусть $V=91$. Заполнение матрицы может быть реализовано последовательным выполнением таких этапов вычислений.

Этап 1. Составим восьмиэлементный регистр (верхняя строка 1 табл. 2), перенумеровав элементы слева направо, начиная с номера 0; вычислим номер элемента $r_1 = V(\mathrm{mod}\, n) = 91_8 = 3$ регистра, в который заносится цифра 1 и этот (третий) элемент затеняется, а во все остальные элементы регистра вписываем 0.

Этап 2. Понижаем на единицу порядок регистра, исключив из предыдущего затененный элемент; вычисляем $r_2 = V(\mathrm{mod}\,(n-1)) = 91_7 = 0$ и затеняем нулевой элемент семибитного регистра.

Продолжая аналогичным образом последующие этапы вычислений, сведем их в табл. 2.

Таблица 2.

Пример алгоритм синтеза перестановочной матрицы восьмого порядка

№ этапа (i)	r_i	Разряды регистра							
1	3	0	1	2	3	4	5	6	7
2	0	0	1	2	3	4	5	6	
3	1	0	1	2	3	4	5		
4	1	0	1	2	3	4			
5	3	0	1	2	3				
6	1	0	1	2					
7	1	0	1						
8	–	0							

По результатам данных табл. 2 легко составить перестановочную матрицу

$$\boldsymbol{P} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Алгебраическая атака матричных протоколов.

Технология организации алгебраической атаки матричных протоколов обмена ключами шифрования предполагает выполнение таких операций:

1) Вычисляются значения векторов

$$\boldsymbol{E}\overline{V},\ \boldsymbol{A}\overline{V},\ \boldsymbol{A}^2\overline{V},\ldots,\ \boldsymbol{A}^{n-1}\overline{V}, \qquad (20)$$

где $\boldsymbol{E}$ – единичная матрица (или матрица $\boldsymbol{A}^0$); $\boldsymbol{A}$ – матрица, параметризируемая открытыми ключами протокола (будет доопределена ниже в рассматриваемых примерах).

2) Определяются коэффициенты $x_0,\ldots,x_{n-1} \in \{0,1\}$ такие, что

$$x_0\boldsymbol{E}\bar{V} + x_1\boldsymbol{A}\bar{V} + x_2\boldsymbol{A}^2\bar{V},\ldots,+x_{n-1}\boldsymbol{A}^{n-1}\bar{V} = \bar{\alpha}\,. \tag{21}$$

3) Вычисляется секретный ключ $\bar{K}$ по формуле

$$\bar{K} = x_0\boldsymbol{E}\bar{\beta} + x_1\boldsymbol{A}\bar{\beta} + x_2\boldsymbol{A}^2\bar{\beta},\ldots,+x_{n-1}\boldsymbol{A}^{n-1}\bar{\beta}\,. \tag{22}$$

Вектор-столбцы $\bar{\alpha}$ и $\bar{\beta}$ в системах матричных уравнений (21) и (22) представляют собою векторы, которыми обмениваются операторы A и B (уточняются далее в числовых примерах протоколов).

Обратимся к иллюстрации результатов алгебраической атаки на протокол Мегрелишвили, выполнив цепочку преобразований (20) – (22). Пусть $n = 5$, $V = 10101$, а секретные ключи $x = 5$ и $y = 6$. Тем самым имеем

$$\bar{V} = \begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix};\quad \boldsymbol{A} = \begin{bmatrix}1&0&1&0&1\\1&1&0&1&0\\0&1&1&0&1\\1&0&1&0&0\\0&1&0&1&0\end{bmatrix},$$

где $\boldsymbol{A}$ есть матрица Мегрелишвили $\boldsymbol{M}$ пятого порядка, ранее составленная в (1).

Общий ключ шифрования $\bar{K}_M$ формируется последовательностью таких шагов. Сначала вычисляются векторы

$$\bar{\alpha} = \boldsymbol{A}^x \cdot \bar{V} = \boldsymbol{A}^5\bar{V} = \begin{bmatrix}0&1&1&1&0\\1&1&1&0&0\\1&1&0&1&1\\1&0&0&0&0\\1&0&1&1&0\end{bmatrix}\cdot\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\\0\end{bmatrix}; \tag{23}$$

и

$$\bar{\beta} = \boldsymbol{A}^y \cdot \bar{V} = \boldsymbol{A}^6\bar{V} = \begin{bmatrix}0&0&0&1&1\\0&0&0&1&0\\1&0&0&0&1\\1&0&1&0&1\\0&1&1&0&0\end{bmatrix}\cdot\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix}, \tag{24}$$

которые дают возможность абонентам A и B вычислить общий ключ шифрования

$$\bar{K}_M = \boldsymbol{A}^{x+y} \cdot \bar{V} = \boldsymbol{A}^{11}\bar{V} = \begin{bmatrix}0&0&1&1&0\\1&0&0&0&0\\1&1&0&0&0\\0&0&0&1&1\\0&0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\\0\end{bmatrix}.$$

Противник на основании априорных данных $\bar{V}$ и $\boldsymbol{A}$ предварительно находит согласно соотношениям (20) векторы

$$\boldsymbol{E}\bar{V} = \begin{bmatrix}1\\0\\1\\0\\1\end{bmatrix}; \quad \boldsymbol{A}\bar{V} = \begin{bmatrix}1\\1\\0\\0\\0\end{bmatrix}; \quad \boldsymbol{A}^2\bar{V} = \begin{bmatrix}1\\0\\1\\1\\1\end{bmatrix}; \quad \boldsymbol{A}^3\bar{V} = \begin{bmatrix}1\\0\\0\\0\\1\end{bmatrix}; \quad \boldsymbol{A}^4\bar{V} = \begin{bmatrix}0\\1\\1\\1\\0\end{bmatrix},$$

а затем, перехватывая кодовые комбинации $\bar{\alpha}$ и $\bar{\beta}$, составляет, с учетом вектор-столбца (23), систему уравнений (21)

$$\begin{bmatrix}x_0\\0\\x_0\\0\\x_0\end{bmatrix} + \begin{bmatrix}x_1\\x_1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}x_2\\0\\x_2\\x_2\\x_2\end{bmatrix} + \begin{bmatrix}x_3\\0\\0\\0\\x_3\end{bmatrix} + \begin{bmatrix}0\\x_4\\x_4\\x_4\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\\0\end{bmatrix},$$

и вычисляет значения

$$x_0 = 1; \quad x_1 = 1; \quad x_2 = 0; \quad x_3 = 1; \quad x_4 = 1.$$

Подставив коэффициенты x_i, $i = \overline{0,4}$, в (22) и принимая во внимание вектор (24), противник определяет ключ

$$\bar{K}_{\alpha\beta} = \begin{bmatrix}1\\0\\0\\1\\1\end{bmatrix} + \begin{bmatrix}0\\0\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\1\\1\\0\end{bmatrix}.$$

Ключ $\bar{K}_{\alpha\beta}$ совпал ключом $\bar{K}_M$, т.е. протокол Мегрелишвили оказывается взломанным.

А теперь рассмотрим предлагаемый альтернативный ОМГ-протокол обмена ключами, полагая $n = 4$ и $f = 10011$. Пусть, кроме того,

$$\bar{V} = \begin{pmatrix}1\\1\\0\\1\end{pmatrix}; \quad \boldsymbol{P} = \begin{pmatrix}0&1&0&0\\0&0&0&1\\1&0&0&0\\0&0&1&0\end{pmatrix}; \quad \boldsymbol{P}^{-1} = \begin{pmatrix}0&0&1&0\\1&0&0&0\\0&0&0&1\\0&1&0&0\end{pmatrix}. \tag{25}$$

В качестве секретных ключей абонентов A и B примем

$$\bar{\omega}_\alpha = \begin{pmatrix}0\\1\\1\\1\end{pmatrix}; \quad \bar{\omega}_\beta = \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \tag{26}$$

однозначно определяющие матрицы Галуа

$$\boldsymbol{G}_a = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}; \qquad \boldsymbol{G}_b = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}. \tag{27}$$

На основании данных (25)-(27) вычисляются векторы $\overline{\alpha}$ и $\overline{\beta}$, которыми обмениваются абоненты A и B,

$$\overline{\alpha} = (\boldsymbol{P} \cdot \boldsymbol{G}_\alpha \cdot \boldsymbol{P}^{-1}) \cdot \overline{V} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \qquad \overline{\beta} = (\boldsymbol{P} \cdot \boldsymbol{G}_\beta \cdot \boldsymbol{P}^{-1}) \cdot \overline{V} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \tag{28}$$

и определяется общий секретный ключ

$$K_c = (\boldsymbol{P} \cdot (\boldsymbol{G}_\alpha \cdot \boldsymbol{G}_\beta) \cdot \boldsymbol{P}^{-1}) \cdot \overline{V} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \tag{29}$$

Противник, пытаясь взломать ключ шифрования K_c, опираясь на априори известный НП f для ОЭ $\omega = 10$ сначала находит матрицу

$$\boldsymbol{A} = \boldsymbol{G}_{f,\omega}^{(4)} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

а также ее степени

$$\boldsymbol{A}^2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}; \quad \boldsymbol{A}^3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

и осуществляет преобразования подобия

$${}^*\boldsymbol{A} = \boldsymbol{P} \cdot \boldsymbol{A} \cdot \boldsymbol{P}^{-1},$$

образуя матрицы

$${}^*\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}; \quad {}^*\boldsymbol{A}^2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}; \quad {}^*\boldsymbol{A}^3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}. \tag{30}$$

Затем противник вычисляет вектор-столбцы

$$ {}^{*}\boldsymbol{A}^{0}\bar{V} = \bar{V} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}; \quad {}^{*}\boldsymbol{A}\bar{V} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}; \quad {}^{*}\boldsymbol{A}^{2}\bar{V} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}; \quad {}^{*}\boldsymbol{A}^{3}\bar{V} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \qquad (31) $$

На основании соотношения (21), векторов (31) и $\bar{\alpha}$ из (28) противник составляет систему линейных уравнений

$$ x_1 \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, $$

решая которую получает коэффициенты

$$ x_1 = 1; \quad x_2 = 1; \quad x_3 = 1; \quad x_4 = 0, $$

а по формуле (22) с учетом значений (24), (28) и (30) вычисляет секретный ключ

$$ \bar{K} = \bar{\beta} + {}^{*}\boldsymbol{A}\bar{\beta} + {}^{*}\boldsymbol{A}^{2}\bar{\beta} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \qquad (32) $$

Из сопоставлений векторов (28) и (32) убеждаемся в том, что алгебраической атакой альтернативный ОМГ-протокол взламывается точно так же просто, как и протокол Мегрелишвили. Кроме того, отметим, что эти протоколы не защищены и от атаки "человек посередине", что, тем ни менее, не снижает их достоинства – возможности применения в системах оперативного обмена ключами шифрования.

Выводы. Сформулируем основные полученные научные результаты. Во-первых, ОМГ-протоколы обмена секретными ключами шифрования по открытым каналам связи могут быть построены для произвольных неприводимых полиномов, тогда как классические матрицы Галуа определяются только над примитивными полиномами. И, во-вторых, каждому примитивному полиному отвечает всего лишь одна единственная примитивная матрица Галуа с образующим элементом $\theta = 10$, в то время как для любого неприводимого полинома f_n, совсем не обязательно являющегося примитивным, число примитивных ОМГ совпадает с числом L_θ примитивных элементов θ поля $GF(2^n)$ над выбранным полиномом f_n, при этом $L_\theta = \varphi(2^n - 1)$, где $\varphi(\cdot) -$ функция Эйлера.

Теоретическая возможность взлома противником ОМГ-протокола алгебраической атакой, которая осуществима лишь при условии априорной определенности относительно открытых ключей и успешного перехвата пакетов V_α и V_β, не создает принципиальных проблем применению его в *аппаратуре специального назначения*, например, для формирования ключей шифрования информации, передаваемой по радиоканалу НПУ – борт БПЛА.

В самом деле, если публичные ключи ОМГ-протокола сделать закрытыми, то тем самым противник будет лишен возможности несанкционированного доступа к каналам передачи данных. Причина такого ограничения заключается в следующем. Поскольку в условиях априорной неопределенности относительно параметров открытых ключей, даже перехватив пакеты V_α и V_β, которыми обмениваются легализованные абоненты A и B,

противник оказывается не в состоянии вычислить их общий секретный ключ шифрования K и, следовательно, ОМГ-протокол оказывактся не взламываемым.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Иран объявил о захвате американского беспилотника. / [Электронный ресурс]. – Режим доступа: http://zn.ua
2. Ивонин М. В. Криптографические протоколы распределения ключей для групп с динамическим составом участников. / М. В. Ивонин. / [Электронный ресурс]. – Режим доступа: http://www.itsecure.org.ua
3. Введение в криптографию: новые математические дисциплины. Учебник под ред. В. В. Ященко. – СПб: Питер, 2001. – 287 с.
4. Diffie W., Hellman M.E. "New Directions in Cryptography", IEEE Transactions on Information Theory, v. IT-22, no. 6, November 1976, 644-654
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. / Б. Шнайер. – М.: "ТРИУМФ", 2003. – 816 с.
6. Ерош И. Л. Адресная передача сообщений с использованием матриц над полем GF (2) / И. Л. Ерош, В. В. Скуратов. // Проблемы информационной безопасности. Компьютерные системы. 2004, №1. – С. 72-78
7. Ерош И. Л. Скоростное шифрование разнородных сообщений / И. Л. Ерош, М. Б. Сергеев. // Проблемы информационной безопасности. 2004. № 1. С. 72-78.
8. Megrelishvili R. Investigation of new matrix-key function for the public cryptosystems. / R. Megrelishvili, M. Chelidze, G. Besiashvili. The Third International Conference "Problems of cybernetics and Information", Volume 1, September 6-8, Baku, Azerbaijan, Section N1, "Information and Communication Technologies", 2010, pp. 75-78.
9. Поточные шифры. Результаты зарубежной открытой криптологии. – М., 1997, 389 с. / [Электронный ресурс]. – Режим доступа: http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm
10. Взломан блочный шифр ГОСТ. / [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/405678.php
11. Однонаправленные функции. / [Электронный ресурс]. – Режим доступа: http:// crypto.pp.ua/2010/06/odnonapravlennye- funkcii/
12. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. / С. Коухтиньо. – Постмаркет, 2007. – 328 с.
13. Регистр сдвига с линейной обратной связью - Википедия. / [Электронный ресурс]. – Режим доступа: https://search.ukr.net/?q= регистр сдвига с линейной обратной связью
14. Муллажонов Р. В. Обобщенное транспонирование матриц и структуры линейных крупномасштабных систем. / Р. В. Муллажонов // Доповіді НАНУ, 2009, № 10. С. 27-35.
15. Гантмахер Ф. Р. Теория матриц. / Ф. Р. Гантмахер. – М.: Физматлит, 2004. – 560 с.
16. Фробениусова нормальная форма. / [Электронный ресурс]. – Режим доступа: Vikipedijya.uz.cm/wiki/Матрица_Фробениуса
17. Подобные матрицы. – Режим доступа: https://ru.wikipedia.org/wiki/Подобные матрицы
18. Golomb S. W. Shift Register Sequences: монография / S. W. Golomb. – San Francisco: Holden Day, 1967. – ISBN 978-3-540-44523-4.
19. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.
20. Однонаправленные функции. / http:// crypto.pp.ua/2010/06/odnonapravlennye_funkcii/

Стаття надійшла до редакції 16.03.16

Білецький А. Я.
Національний авіаційний університет, Київ, Україна

УЗАГАЛЬНЕНІ МАТРИЦІ ГАЛУА В ПРОТОКОЛАХ ОБМІНУ КЛЮЧАМИ ШИФРУВАННЯ

Розглянуто методи побудови матричних протоколів формування секретних ключів шифрування легалізованими абонентами відкритих комунікаційних мереж. В основу

протоколів обміну ключами покладені алгоритми асиметричної криптографії. Рішення проблеми передбачає обчислення односторонніх функцій і базується на використанні узагальнених матриць Галуа, пов'язаних відношенням ізоморфізму з утворюючими елементами, і залежать від обраних незвідних поліномів, що породжують матриці. Розроблено простий спосіб побудови узагальнених матриць Галуа за методом діагонального заповнення. З метою усунення ізоморфізму матриць Галуа і утворюючих їх елементів, що обмежує можливість побудови односторонніх функцій, матриці Галуа піддаються перетворенню подібності, здійснюваних за допомогою перестановочних матриць. Пропонується варіант організації алгебраїчної атаки на протоколи обміну ключами шифрування і обговорюються варіанти ослаблення наслідків атаки.

Ключові слова: протокол обміну ключами, односторонні функції, узагальнені матриці Галуа, відношення ізоморфізму, алгебраїчна атака на протокол обміну ключами шифрування.

Anatoly Beletsky
National Aviation University, Kiev, Ukraine

GENERALIZED MATRIXES OF GALOIS PROTOCOLS EXCHANGE ENCRYPTION KEYS

The methods of construction of matrix formation the secret protocols legalized subscribers of public communications networks encryption keys. Based key exchange protocols laid asymmetric cryptography algorithms. The solution involves the calculation of one-way functions and is based on the use of generalized Galois arrays of isomorphism relationship with forming elements, and depending on the selected irreducible polynomial generating matrix. A simple method for constructing generalized Galois matrix by the method of filling the diagonal. In order to eliminate the isomorphism of Galois arrays and their constituent elements, limiting the possibility of building one-way functions, Galois matrix subjected to similarity transformation carried out by means of permutation matrices. The variant of the organization of the algebraic attacks on encryption keys sharing protocols and discusses options for easing the consequences of an attack.

Keywords: key exchange protocol, one-way functions, generalized Galois matrix ratio isomorphism, algebraic attack on the encryption key exchange protocol.